CNIL
Commission Nationale de l'Informatique et des Libertés

Club EBIOS

Réunion Mardi 3 novembre de 14h à 17h

SIV/SIIV

RAPPEL - But de cet échange :

- Contexte
- Préciser quels sont les risques
- Quelles sont les bonnes pratiques ou les enjeux méthodologiques dans la prise en compte de ces risques

Source de menaces / Directive Nationale de Sécurité (DNS)

Une directive nationale de sécurité s'applique à tout ou partie d'un secteur d'activités d'importance vitale. Elle **décrit le périmètre du secteur** ou du sous-secteur, elle en identifie les **responsables** et les **enjeux** et en définit le **besoin de sécurité**.

A la suite d'une analyse de risque dans laquelle sont énoncés et hiérarchisés **les scénarios de menace**, elle précise les objectifs et les politiques de sécurité du secteur ou de la partie de secteur concerné.

A cette fin, la directive nationale de sécurité peut notamment définir la nature des opérateurs et des infrastructures susceptibles d'être désignés d'importance vitale au titre dudit secteur et préciser les critères de leur désignation. La directive nationale de sécurité définit des mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute **menace**, notamment à caractère terroriste (N° 6600/SGDN/PSE/PPS du 26 septembre 2008).

Menaces

- actes malveillants (Etats, personnels internes, pirates, crime organisé) ou terroristes,
- les risques naturels et technologiques

La loi de programmation militaire appliquée à la cybersécurité

Cinq articles de la LPM 2014-2019 traitent de sujets cyber. Tout d'abord, dans le chapitre III : « **Dispositions relatives au renseignement** »,

- l'article 20 relatif à « **l'accès administratif aux données de connexion**» (annexes 2 et 4).

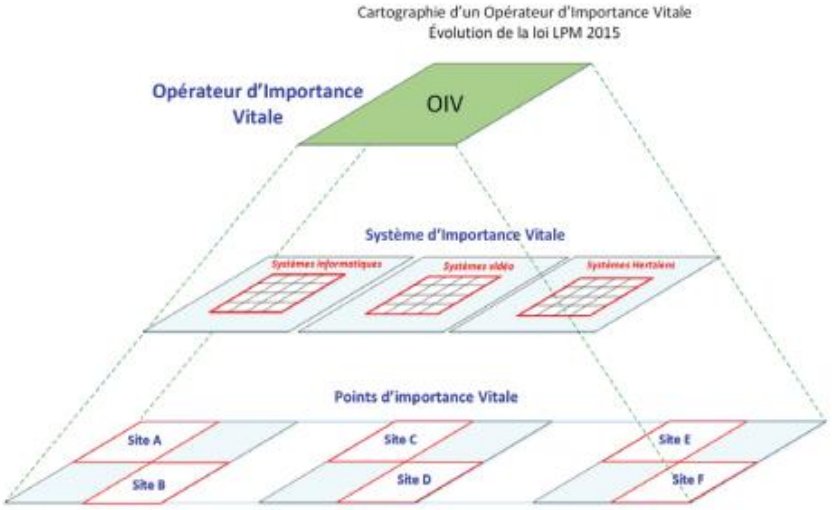
Puis les articles 21, 22, 23 et 24 qui font parties du chapitre IV: « Dispositions relatives à la protection des infrastructures vitales contre la **cybermenace**» (annexe 3):

- L'article 21: redéfinit les responsabilités et les actions possibles en matière de cybersécurité en modifiant le code de la défense.
- L'article 22: désignation, responsabilités et obligations des OIV en termes de protection de leurs installations (**sondes de détection, audit, prestataires qualifiés**).
- L'article 23: est relatif à l'utilisation non autorisée de dispositifs d'interception ou d'écoute par voie électronique.
- L'article 24: est relatif à la protection et l'utilisation des données personnelles et de localisation.

OIV et Art.22 LPM

❖ La **LPM** s'applique aux **Organismes d'importance vitale** (OIV) définis dans les articles L1332-1 et 2 du Code de la défense.

❖ **Art.22** de la LPM : responsabilités et obligations des **OIV** en termes de protection de leurs installations. Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, sont tenus de coopérer à leurs frais, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste.



SIIV – Système d'information d'importance vitale

Le Système d'information d'importance vitale est l'élément principal du dispositif défini par la LPM.

Les SIIV participent à un processus vital de l'opérateur. Un processus est appelé «**processus vital**» **lorsqu'au moins une des activités le composant est nécessaire à la réalisation d'une des missions vitales notifiées à l'opérateur**.

Un système d'information d'importance vitale est un SI «**pour lequel l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique ou la capacité de survie de la Nation** » (cf. article L.1332-6-1 du Code de la défense nationale), ainsi que les SI pour lesquels l'atteinte à la sécurité «**pourrait présenter un danger grave pour la population** » (cf. article L.1332-2 du Code de la défense national).

Seront définis comme **SIIV parmi les SI ceux qui supportent les processus vitaux**, ceux pour lesquelles une atteinte à la disponibilité, à la confidentialité ou à l'intégrité pourrait avoir un impact important pour l'OIV (le niveau d'impact étant défini par l'OIV). Sont aussi à considérer comme SIIV, les SI dont le dysfonctionnement au-delà d'une certaine période : – conduit l'opérateur à ne plus pouvoir satisfaire à des obligations définies avec leur modalité d'exécution, soit dans un contrat de service public, soit de façon légale ou réglementaire ; – provoque des conséquences financières pouvant compromettre gravement la situation économique de l'opérateur et par voie de conséquence compromettre la réalisation des missions vitales qui lui ont été notifiées. Le décret n°2015-351 du 27 mars 2015 prévoit que les OIV établissent la liste de leurs SIIV, sur la base de critères fixés dans les arrêtés sectoriels, et la transmettent à l'ANSSI.

Risques d'applicabilité

4 risques majeurs d'applicabilité ont été identifiés

❖ Risque sur les **délais** de mise en œuvre des mesures exigées par l'ANSSI qui pourraient être incompatibles avec les cycles de régénération des systèmes industriels des OIV.

❖ Risque de **soutenabilité** de la démarche compte tenu de la portée financière et organisationnelle de ces mesures à estimer (des coûts récurrents importants déjà identifiés).

❖ Risque sur l'**impossibilité technique** à sécuriser des systèmes existants trop obsolètes pour appliquer les règles ANSSI sans une réingénierie complète.

❖ **Risque d'exploitation et de maintien en condition de sécurité des systèmes dans la durée**. Les mesures techniques de maintien en condition de sécurité sont particulièrement contraignantes pour des systèmes informatiques industriels ayant une longévité difficilement compatibles avec l'évolution rapide des technologies informatiques et de télécommunication.

Analyse des impacts de la LPM

❖ **Légal** : comment appliquer les différents articles sans être hors la loi, dépasser les limites fixées par la LPM ou simplement l'incompatibilité avec l'OIV (**politique de gestion des brevets, production, gestion RH, structuration du SI**, etc.)

❖ **Organisationnel** : il faut que l'organisation interne des OIV soit modifiée et adaptée pour répondre aux différentes contraintes de la LPM (**gouvernance, maitrise des risques, gestion de crise, plan de formation**, etc.)

❖ **Technologique** : selon les directives de la LPM, une diversité des technologies va être déployée pour répondre aux différentes prescriptions, gestion du changement au niveau technique (**analyse des SI et maitrise des risques, systèmes d'alerte et de reporting**, etc.)

❖ **Financier** : la mise en œuvre a un coût associé aux modifications d'organisation, à la mise en place des nouveaux dispositifs techniques, leur exploitation, et leur contrôle (**le coût de l'organisation, le coût de la technique, le coût de la non conformité**, etc.)

Mise en œuvre des mesures de protection des SIIV

Historiquement, le dispositif **SAIV** avait prévu dès le départ la notion de «**point d'importance vitale** » (**PIV**) des opérateurs et des plans de protection de ces PIV. En introduisant la notion de SIIV, le paradigme change un peu : la protection doit s'appliquer non plus à un point mais sur un système potentiellement diffus et éventuellement réparti.

Cela nécessite une appréhension un peu différente de la conception des protections de ces composants. Dans la démarche, les fondamentaux demeurent valides :

- L'aspect **protection physique** (sécurisation physique périmétrique anti intrusion, limitation et traçabilité des accès, protection électrique, climatique et redondance télécoms)
- L'aspect **protection Logique** (confidentialité et intégrité des données, disponibilité, traçabilité, non répudiation)
- L'aspect **RH** (probité et fiabilité des personnes habilitées, contrats de sous-traitance)